UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/839,300	04/23/2001	Yuefeng Liu	6502.0333	3107

60667 7590 04/08/2008

SUN MICROSYSTEMS/FINNEGAN, HENDERSON LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
NGUYEN, PHUONGCHAU BA	
ART UNIT	PAPER NUMBER
2616	
MAIL DATE	DELIVERY MODE
04/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/839,300	LIU, YUEFENG	
	Examiner	Art Unit	
	PHUONGCHAU BA NGUYEN	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *AF 3-15-8*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26 and 37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26, 37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-26 and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Caronni (7,336,790).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

Regarding claim 1,

Caronni (7,336,790) discloses a method for communicating between a first private network (a VPN1-not shown, or could be enterprise network 102) and a second private network (superNet-not shown) configured from nodes (i.e., 301, 304, 312-fig.3) in a public network, comprising:

receiving a non-tunneled packet from a source node in the first private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a destination node in the second private network and acquiring a channel key associated with a channel based on the determination (step 606-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

forwarding the packet over the channel to the destination node (col.5, lines 16-17).

Regarding claim 2,

Caronni further discloses said forwarding comprising: sending the packet to the destination node using the address mapping, the address mapping reflecting a relationship between an internal address for the destination node for use in communicating among nodes in the second private network and an external address for the destination node suitable for communicating over the public network (steps 606-608).

Regarding claim 3,

Caronni further discloses said sending further comprising, adding the external address (new member's virtual address, col.9, lines 11 & 61) to the packet.

Regarding claim 4,

Caronni further discloses said sending further comprising, encrypting the packet (col.9, lines 41-42).

Regarding claim 5

Caronni further discloses said obtaining comprising, accessing the address mapping based on a determination that the packet is destined for the second private

network (steps 604-606-fig.6A, joining supernet).

Regarding claim 6,

Caronni further discloses said determining comprising, determining whether an address mapping exists for a destination address in the packet (step 604-fig.6A).

Regarding claim 7,

Caronni discloses a method for communicating between a first private network (VPN1-i.e., enterprise network, fig.1) and a second private network (supernet) configured from nodes in a public network, comprising:

receiving a non-tunneled packet from a source node in the first private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a destination node in the second private network (step 606-fig.6A), and acquiring a channel key associated with a channel based on the determination (step 610-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

sending the packet over the channel to the destination node (col.5, lines 16-17) using the address mapping, the address mapping reflecting a relationship between an internal address for the destination node for use in communicating among nodes in the second private network and an external address for the destination node suitable for communicating over the public network (steps 606-608).

Regarding claim 8,

Caronni discloses a method for communicating between a first private network (enterprise network) and a second private network (supernet)that uses a public network infrastructure, comprising:

receiving a non-tunneled packet from a source node in the second private network(step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a router node in the first private network (step 606-fig.6A), and acquiring a channel key associated with a channel based on the determination (step 610-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the router node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

forwarding the packet over the channel to a destination node in the first private network (col.5, lines 16-17).

Regarding claim 9,

Caronni further discloses said forwarding comprising: sending the packet to the router node using the address mapping, wherein the router node forwards the packet to the destination node based on an internal address in the packet for the destination node suitable for communicating among nodes in the first private network (steps 606-608, fig.6A).

Regarding claim 10,

Caronni further discloses said sending further comprising,

adding, to the packet, an external address for the router node suitable for communicating over the public infrastructure (new member's virtual address, col.9, lines 11 & 61).

Regarding claim 11,

Caronni further discloses said sending further comprising, encrypting the packet (col.9, lines 41-42).

Regarding claim 12,

Caronni further discloses said obtaining comprising, accessing the address mapping based on a determination that the packet is not destined for the second private network (steps 604-606, fig.6A, joining supernet).

Regarding claim 13,

Caronni further discloses said determining comprising, determining whether an address mapping exists for a destination address in the packet (step 604-fig.6A).

Regarding claim 14,

Caronni discloses a method for communicating between a first private network and a second private network that uses a public network infrastructure, comprising:

receiving a non-tunneled packet from a source node in the second private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a router node (step 606-fig.6A), and acquiring a channel key associated with a channel based on the determination (step 610-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the router node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

sending the packet over the channel to the router node using the address mapping (col.5, lines 16-17). wherein the router node forwards the packet to a destination node in

the first private network based on an internal address in the packet for the destination node suitable for communicating among nodes in the first private network (steps 6060-608-fig.6A).

Regarding claim 15,

Caronni discloses an apparatus for communicating between a first private network and a second private network that uses a public network infrastructure, comprising:

a memory having program instructions; and

a processor responsive to the program instructions to:

receive a non-tunneled packet from a source node in the first private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2),

determine whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added),

acquire a channel key associated with a channel based on the determination (step 610-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source

node and a destination node in the second private network (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel(col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

forward the packet over the channel to the destination node (col.5, lines 16-17).

Regarding claim 16,

Caronni discloses an apparatus for communicating between a first private network and a second private network that uses a public network infrastructure, comprising:

a memory having program instructions (col.8, line 63-col.9, line5); and

a processor responsive to the program instructions to:

receive a non-tunneled packet from a source node in the second private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2),

determine whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added), and

acquire a channel key associated with a channel based on the determination,

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and a destination node in the first private network (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel, [[and]]

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

forward the packet over the channel to the destination node (col.5, lines 16-17).

Regarding claim 17,

Caronni discloses a tangible computer-readable storage medium containing instructions (col.8, line 63-col.9, line5) which, when executed by a processor, perform a method for communicating between a first private network and a second private network that uses a public network infrastructure, the method comprising:

receiving a non-tunneled packet from a source node in the first private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a destination node in the second private network (step 606-fig.6A), and acquiring a channel key associated with a channel based on the determination (step 610-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the destination node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45),l, and wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

sending the packet over the channel to the destination node using the address mapping (col.5, lines 16-17), the address mapping reflecting a relationship between an internal address for the destination node for use in communicating among nodes in the second private network and an external address for the destination node suitable for communicating over the public infrastructure (steps 606-608-fig.6A).

Regarding claim 18,

Caronni further discloses said sending further comprising, adding the external address to the packet (new member's virtual address, col.9, lines 11 and 61).

Regarding claim 19,

Caronni further discloses said sending further comprising, encrypting the packet (col.9, lines 41-42).

Regarding claim 20,

Caronni further discloses said obtaining comprising, accessing the address mapping based on a determination that the packet is destined for the second private network (steps 604-606, fig.6A, joining supernet).

Regarding claim 21,

Caronni further discloses said determining comprising, determining whether an address mapping exists for a destination address in the packet (step 604, fig.6A).

Regarding claim 22

Caronni discloses a tangible computer-readable storage medium containing instructions which, when executed by a processor (col.8, line 63-col.9, line5),

perform a method for communicating between a first private network and a second private network that uses a public network infrastructure, the method comprising:

receiving a non-tunneled packet from a source node in the second private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a router node (step 606-fig.6A), and acquiring a channel key associated with a channel based on the determination (step 610-fig.6A),,

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the router node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45); and

sending the packet over the channel to the router node using the address mapping (col.5, lines 16-17), wherein the router node forwards the packet to a destination node in the first private network based on an internal address in the packet for the destination

node suitable for communicating among nodes in the first private network (steps 606-608-fig.6A).

Regarding claim 23,

Caronni further discloses said sending further comprising, adding, to the packet, an external address for the router node suitable for communicating over the public infrastructure (new member's virtual address, col.9, lines 11 & 61)).

Regarding claim 24,

Caronni further discloses said sending further comprising, encrypting the packet (col.9, lines 41-42).

Regarding claim 25,

Caronni further discloses said obtaining comprising, accessing the address mapping based on a determination that the packet is not destined for the second private network (steps 604-606, fig.6A, joining supernet).

Regarding claim 26,

Caronni further discloses said determining comprising, determining whether an address mapping exists for a destination address in the packet (step 604, fig.6A).

Claims 27-36. (Cancelled).

Regarding claim 37.

(Previously Presented) A method for communicating between a first private network and a second private network configured from nodes in a public network, comprising:

receiving, at a router node, a first non-tunneled packet from a source node in the first private network, wherein the router node facilitates connection between the first private network and the second private network (step 602-fig.6A, when a node from a VPN1 joining a Supernet-VPN2);

determining whether the first packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to a second destination node in the second private network and acquiring a channel key associated with a channel based on the determination (step 606-fig.6A),

wherein the channel comprises a plurality of non-tunneled virtual links (a collection of virtual links, col.5, lines 11-15) through the public network that connects a plurality of channel nodes, the channel nodes including the source node and the router node (fig.4, channel having nodes),

wherein only the channel nodes are permitted to communicate over the channel (col.5, lines 11-23 & see also fig.4),

wherein the channel key is updated upon an addition of a new channel node to the channel (col.5, lines 53-56; col.9, lines 42-45), and

wherein the channel key is updated upon a departure of one of the channel nodes from the channel (col.5, lines 53-56; col.9, lines 42-45);

sending the first packet over the channel to the second destination node using the address mapping (steps 606-608, fig.6A), the address mapping reflecting a relationship between an internal address for the second destination node for use in communicating among nodes in the second private network and an external address for the second destination node suitable for communicating over the public infrastructure;

receiving a second non-tunneled packet from a source node in the second private network (step 602-fig.6A, when another node from a VPN1 joining a Supernet-VPN2);

determining whether the second packet is destined for the second private network (step 602-fig.6A, validated ID and password for Supernet-emphasis added);

obtaining an address mapping corresponding to the router node based on the determination that the second packet is not destined for the second private network (step 606-fig.6A); and

sending the packet over the channel to the router node using the address mapping corresponding to the router node (col.5, lines 16-17), wherein the router node forwards the packet to a first destination node in the first private network based on an internal address in the second packet for the first destination node suitable for communicating among nodes in the first private network (steps 606-608-fig.6A).

Allowable Subject Matter

3. The indicated allowability of claims 1-26, 37 is withdrawn in view of the newly discovered reference(s) to Caronni (7, 336,790). Rejections based on the newly cited reference(s) follow.

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Caronni (6,938,169) and Matsumoto (6215877).

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHUONGCHAU BA NGUYEN whose telephone number is (571)272-3148. The examiner can normally be reached on Monday-Thursday from 8:30 a.m. to 7:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on 571-272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PHUONGCHAU BA NGUYEN/
Examiner, Art Unit 2616

/Huy D. Vu/

Supervisory Patent Examiner, Art Unit 2616